TEXAS
Health and Human Services

HHS CIRCULAR C-021
HEALTH AND HUMAN SERVICES SYSTEM
INFORMATION SECURITY/CYBERSECURITY POLICY

Purpose

The purpose of this policy is to establish the authority, role, and responsibility of health and human services (HHS) system Information Security for:

- maintaining an information security program;
- overseeing the information security function system-wide; and,
- establishing authority at the agency levels for implementing the system Information Security objectives.

"Security" in this document is defined as protecting the confidentiality, integrity, and availability of business essential information for both internal and external customers, who have a bona fide business need to access that information.

This policy is provided as a measure and means of layered accountability to protect HHS system information resources against unauthorized access, disclosure, modification, or destruction, as well as to ensure the availability, integrity, utility, authenticity, non-repudiation, and confidentiality of information. For the purpose of the security program, the word "enterprise" is synonymous with "system."

Directive

The HHS Executive Commissioner or his/her designee:

- Directs the HHS Chief Information Security Officer (CISO) and system Information Security Office to develop and maintain the HHS system Information Security program that consists of system-wide security policies, standards, controls, guidelines and procedures which meet all state laws and federal requirements.
- Directs the HHS system Information Security Office to oversee the security functions system-wide. The security functions include, but are not limited to: security risk management, incident management, investigations, analysis, assessments, monitoring, awareness, training, consulting, and the usage of security tools and system security accounts.
- Directs each agency's Information Security Officer (ISO) to report to the system CISO. The ISO will also have a formal relationship with their respective agency's executive management. Each HHS agency information security office is an extension of the system

program and security objectives. In addition, each agency ISO will be responsible for the specifics of their agency's security program where they will work with their respective agency's executive management to establish annual plans and address the security needs of that agency.

- Authorizes the CISO to approve exceptions to system information security requirements based on documented justifications, compensating controls, and an establishment of a review cycle.

Scope

This policy applies to all authorized network users including, but not limited to, HHS system personnel, temporary employees, interns, volunteers, trainees, employees of independent contractors, and guests of HHS' system information resources, regardless of level of privilege.

Enforcement

- Users who violate this policy will be subject to loss of access to information resources.
- Employees of the HHS system may be subject to disciplinary action in accordance with Chapter 4, Employee Conduct, Chapter 10, Performance and Contract Management, and Chapter 11, Disciplinary Actions, of the HHS Human Resources Manual.

Policy

The policy of the HHS system is as follows:

- The HHS CISO will collaborate with the agency ISOs for developing and implementing the HHS System Information Security (SIS) program. The SIS program will consist of information security plans, policies, standards, controls, guidelines, and procedures that apply to the HHS system.
  - The CISO will collaborate with the HHS Chief Privacy Officer to develop the system incident response framework, of which the security incident response plan is a component; collaborate on investigations involving both privacy and security issues; and will be a standing member of the HHS Incident Response Team. The CISO will collaborate with the HHS Chief Privacy Officer on governance over safeguarding confidential information.
  - The Enterprise Information Security (EIS) policy will contain the program's security policies, which will be approved through the HHS governance structure.
  - The Enterprise Information Security Standards and Guidelines (EISSG) will contain security standards, controls, and guidelines related to technology and processes. Because technology and processes change rapidly, flexibility for updating this document is necessary. Therefore, additions and revisions made to the EISSG will be managed collaboratively at the HHS agency ISO level and submitted to the HHS CISO for final approval.

  - A System Information Security (SIS) plan containing the executive update of the security plans, risks, and effectiveness of the SIS program will be maintained.
- HHS agencies may further develop and implement information security policies, standards, controls, guidelines, procedures, and plans for their agencies that are consistent with and will not limit the effectiveness or requirements of the SIS program.

Responsibilities

The HHS Executive Commissioner or his/her designee will designate the HHS system CISO, who will also be responsible for the HHSC Information Security program.

The HHS Executive Commissioner and each agency Commissioner or his/her designee will:

- Enforce this policy.
- Hold senior management accountable for compliance with this policy.
- Designate an agency ISO who, in cooperation with the HHS CISO, will administer the system and agency Information Security program.
- Provide funding support for the system Information Security program functions.
- Review and approve the agency's Information Security program.

The Deputy Executive Commissioner for Information Technology & CIO will:

- Advocate to ensure that the system Information Security program functions are appropriately funded.
- Advocate to ensure that the system and agency Information Security programs are staffed appropriately to successfully execute program initiatives.
- Ensure that high-risk program initiatives are communicated to the Executive Commissioner or his/her designee.

The Chief Information Security Officer (CISO) will:

- Provide leadership, direction, and coordination for the HHS SIS program.
- Maintain the HHS SIS program, which is a risk-based and collaborative effort among the HHS agency ISOs and other stakeholders.
- Explore, recommend, and implement system security strategies, tools, and resources for HHS efficiencies.
- Monitor and report on the compliance and effectiveness of system security strategies.
- Establish an Information Security Associate (ISA) program for communicating, training, and delegating security responsibilities throughout the system.
- Develop and implement a comprehensive, system-wide training and awareness program.

- Develop, implement, maintain, and manage security defense in depth strategies that protect from unauthorized IT intrusions and immediately responds to and mitigates unauthorized access and data compromise.

Each agency ISO shall:

- Manage agency specific security issues, events and incidents, including escalation, and keep agency management and the CISO informed.
- Communicate their agency's information security needs to the CISO.
- Collaborate on, provide input to, and actively participate in the SIS program.
- Administer the system and agency information security programs.
- Implement procedures and practices aligned with the SIS program to ensure the security of information resources.
- Establish procedures for assessing and ensuring compliance with information security policies through inspections, reviews, and evaluations.
- Establish an agency Information Security Training and Awareness program, which compliments the system initiatives.
- Work collaboratively with the agency to develop, maintain, and execute an agency-wide information security plan as required by Government Code §2054.133.
- Work with the business and technical resources to ensure that security controls are utilized to address all applicable requirements.
- Provide guidance and assistance to senior agency officials, information owners, information custodians, and end users concerning their responsibilities.
- Ensure that annual information security risk assessments are performed and documented by information owners.
- Review and annually update the agency's inventory of information systems and related ownership and responsibilities.
- Review and update or respond to the data security requirements, specifications and, if applicable, third-party risk assessments of any new computer applications or services that receive, maintain, and/or share confidential information.
- Verify that appropriate security and privacy requirements are in place for the purchase of required information technology hardware, software, and systems development services for any new mission critical computer applications or computer applications that receive, maintain, and/or share confidential data.
- Monitor the compliance and effectiveness of defined security controls.
- Report on the status and effectiveness of information resources security controls.
- Serve as the agency's internal and external point of contact for all information security matters.
- Issue exceptions that may be needed to information security requirements or controls, with the approval of the HHS agency Commissioner. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.

- Provide the CISO reports relating to their agency’s information security plans, status, and effectiveness including, but not limited to:
  - DIR required reporting;
  - annual program plans, as provided to their agency heads;
  - compliance status; and,
  - required metrics illustrating program effectiveness.

Procedures

The attached HHS EIS policy provides a framework for the protection of HHS information resources.

Inquiries

Inquiries regarding the content of this circular should be directed to the system Information Security Office at InfoSecurity@hhsc.state.tx.us or to the CISO at (512) 438-2091.